## ABSTRACT

Systems and methods for negotiating an encryption algorithm may be implemented in the context of encryption-based authentication protocols. The invention has the added benefit of providing a system an method that need not interfere with the standard operation of authentication protocols. A first computer, or client computer, can send a negotiation request to a second computer, or server computer. The negotiation request can specify that the client computer supports a selected encryption algorithm. In response, the server computer can return a subsession key for encryption using the selected encryption algorithm. Both client and server may then switch to encryption in the selected encryption algorithm, using the subsession key to encrypt future communications.